CSCE604243 Kriptografi & Keamanan Informasi

Semester Genap 2019/2020

Deskripsi Tugas Kelompok Kriptanalisis:

1. Setiap kelompok diberikan satu topik cryptanalysis secara random dan petunjuk umum (misal: contoh kode atau paper).
2. Setiap kelompok menulis satu bab pada rangkuman buku teknik cryptanalysis yang berisi deskripsi algoritma kriptografi dan teknik cryptanalysis yang digunakan (rangkuman ditulis menggunakan latex dengan template yang ditentukan). Masing-masing kelompok mesti menggali dan menambahkan sendiri referensi dan contoh kode yang digunakan.
3. Setiap kelompok mengimplementasikan teknik cryptanalisis yang digunakan menggunakan python murni dan mengupload kode ke gitlab.cs.ui.ac.id dan menuliskan linknya di scele
4. Setiap kelompok mempresentasikan dan mendemokan hasil tugas kelompok sesuai dengan jadwal yang sudah ditentukan

Daftar Proyek Kriptanalisis:

1. Serangan terhadap Vigenere cipher untuk pesan bahasa Indonesia (contoh kode: https://github.com/cbornstein/python-vigenere)
2. Serangan terhadap 3 ronde DES (contoh kode: https://github.com/twhiteman/pyDes) - https://lirias.kuleuven.be/retrieve/333520
3. Serangan Padding Oracle untuk CBC (contoh kode: https://github.com/TheCrowned/padding-oracle-attack)
4. MD5 collision attack (http://crppit.epfl.ch/documentation/Hash_Function/Examples/Code_Project/Documentation/104.pdf)
5. Common modulus attack (https://eprint.iacr.org/2009/037.pdf) - https://github.com/eazebu/RSAExploits
6. Index calculus Attack to discrete log (https://github.com/davidcox143/pyDLP)
7. Attack to elliptic curve (https://github.com/tintinweb/ecdsa-private-key-recovery)
8. Attack to TLS protocol (https://github.com/mpgn/BEAST-PoC)